UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/600,687	06/20/2003	Philip D. MacKenzie	15	6727

7590 01/21/2010

Ryan, Mason, & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560

EXAMINER	
TO, BAOTRAN N	
ART UNIT	PAPER NUMBER
2435	
MAIL DATE	DELIVERY MODE
01/21/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/600,687
Filing Date: June 20, 2003
Appellant(s): MACKENZIE, PHILIP D.

David E. Shifren
Reg. No. 59,329
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 10/14/2009 appealing from the Office action mailed 06/15/2009.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,697,488	CRAMER	02-2004
5,515,441	FAUCHER	05-1996

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1-2, 4-6, 8-9-10, 12-14, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cramer et al, (US Patent No. 6,697,488) hereinafter Cramer in view of Faucher (US Patent No. 5,515,441) hereinafter Faucher.

As per claims 1 and 9, Cramer discloses a method for use in a device associated with a first party for decrypting a ciphertext according to a Cramer-Shoup based encryption scheme (Col. 6 lines 10-15), the method comprising the steps of:

obtaining the ciphertext in the first party device sent from a device associated with a second party (Col. 8, lines 25-35, encrypted plaintext); and

generating in the first party device a plaintext corresponding to the ciphertext based on assistance from the second device, the plaintext representing a result of the decryption according to the Cramer-Shoup based encryption scheme (Col. 8 line 25 to Col. 10 line 5) { Section IV teaches a verification steps to check the received ciphertext. Section V teaches steps of decrypting the received and verified ciphertext with the assistance of the sender} (Cramer and Shoup cryptographic system invention).

Cramer does not disclose "wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device, such that the first party device and the second party device jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party hold, but such that either can decrypt the ciphertext alone."

However, Faucher explicitly discloses wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device (col. 3, lines 5-50), such that the first party device and the second party device jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party hold, but such that either can decrypt the ciphertext alone (Figure 5, col. 8, lines 8-55).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Faucher's reference within Cramer to include wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device, such that the first party device and the second party device jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party hold, but such that either can decrypt the ciphertext alone. One of ordinary skill in the art would have been motivated to do this because it would secure communications conducted over insecure channels using pubic-keys method (col. 1, lines 13-15).

As per claims 8 and 16, Cramer discloses a method for use in a device associated with a first party for assisting in decrypting a ciphertext according to a Cramer-Shoup based encryption scheme, the method comprising the steps of:

receiving a request generated in and transmitted by a second party device for the partial assistance {*the partial assistance is the steps to verify the ciphertext before going through the decryption process in section V*} of the first party device in decrypting the ciphertext according to the Cramer-Shoup based encryption scheme (Col. 8, line 38 – Col. 9, line 25); and

generating results in the first party device based on the partial assistance provided thereby for use in the second party device to complete decryption of the ciphertext" (Col. 8 line to Col. 10 line 5) { *Section IV teaches a verification steps to check the received ciphertext. Section V teaches steps of decrypting the received and verified ciphertext with the assistance of the sender*} (*Cramer and Shoup are the inventors of this prior art*) (Col. 8 line 25 to Col. 10 line 5).

Cramer does not disclose "wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device, such that the first party device and the second party device jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party hold, but such that either can decrypt the ciphertext alone."

However, Faucher explicitly discloses wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device (col. 3, lines 5-50), such that the first party device and the second party device jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party hold, but such that either can decrypt the ciphertext alone (Figure 5, col. 8, lines 8-55).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Faucher's reference within Cramer to include wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device, such that the first party device and the second party device jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party hold, but such that either can decrypt the ciphertext alone. One of ordinary skill in the art would have been motivated to do this because it would secure communications conducted over insecure channels using pubic-keys method (col. 1, lines 13-15).

As per claims 2 and 10, the combination of Cramer and Faucher discloses the limitations of Claims 1 and 9. Faucher further discloses wherein the generating step further

comprises an exchange of information between the first party device and the second party device whereby at least a portion of the information is encrypted using an encryption technique such that one party encrypts information using its own public key and another party can not read the information but can use the information to perform an operation" (Faucher, Figure 5, col. 8, lines 8-55).

As per claims 4 and 12, the combination of Cramer and Faucher discloses the limitations of Claims 1 and 9. Cramer further discloses wherein the generating step further comprises:

generating a share of a random secret (Col. 7, lines 11-19);

generating information representing encryptions of a form of the random secret, a share of a private key, and the ciphertext (Col. 7 lines 10-27) {private key Z, and the random group};

transmitting at least the encrypted information to the second party device (Col. 6, lines 46-57); and

computing the plaintext based at least on the share of the random secret, the share of the private key, the ciphertext, and the data received from the second party device (Figure 3, Col. 9 lines 25-50).

As per claims 5 and 13, the combination of Cramer and Faucher discloses the limitations of Claims 1 and 9. Cramer further discloses wherein the first party device and the second party device additively share components of a private key" in (Col. 7 lines 10-15, and Col. 9 lines 35-40).

As per claims 6 and 14, the combination of Cramer and Faucher discloses the limitations of Claims 1 and 9. Cramer further discloses wherein the generating step further comprises generation and exchange of proofs between the first party device and the second party device that serve to verify operations performed by each party" in (Col. 8 line 38 to Col. 9 line 23).

2. Claims 3, 7, 11, and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cramer and Faucher and further in view of Ronald Cramer et al, "Multiparty Computation from Threshold Homomorphic Encryption".

As per claims 3 and 11, the combination of Cramer and Faucher discloses the limitations of Claims 1 and 9. The combination of Cramer and Faucher does not disclose "wherein the generating step further comprises an exchange of information between the first party device and the second party device whereby at least a portion of the information is encrypted using an encryption technique having a homomorphic property."

However, Ronald Cramer discloses wherein the generating step further comprises an exchange of information between the first party device and the second party device whereby

at least a portion of the information is encrypted using an encryption technique having a homomorphic property (page 18).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Ronald Cramer's reference within Cramer and Faucher to include the encryption technique having a homomorphic property. One of ordinary skill in the art would have been motivated to do this because it would secure communications conducted over insecure channels (col. 1, lines 13-15).

As per claims 7 and 15, the combination of Cramer and Faucher discloses the limitations of Claims 1 and 9. The combination of Cramer and Faucher does not disclose wherein the proofs are consistency proofs based on three-move SIGMA-protocols.

However, Ronald Cramer discloses wherein the proofs are consistency proofs based on three-move SIGMA-protocols the proofs are based on three move SIGMA. Protocols (page 13).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Ronald Cramer's reference within Cramer and Faucher to include the proofs are based on three move SIGMA. protocols. One of ordinary skill in the art would have been motivated to do this because it would secure communications conducted over insecure channels (col. 1, lines 13-15).

(10) Response to Argument

I. Regarding independent Claims 1, 8, 9, and 16,

Appellant appears to argue that "the Faucher protocol is a key exchange and not a decryption operation" (Page 8 of Remarks).

This is not found persuasive because Faucher explicitly discloses the decryption operation in Figure 5 and col. 8, lines 25-47 "**Terminal A generates a secret random component R.sub.a, calculates the corresponding public component X.sup.R.sbsp.a mod P, encrypts it using the public encryption key PK.sub.b extracted from terminal B's certificate, and transmits PK.sub.b (X.sup.R.sbsp.a mod P) to terminal B**. Terminal B generates a secret random component R.sub.b, calculates the corresponding public component X.sup.R.sbsp.b mod P, encrypts it using the public encryption key PK.sub.a extracted from terminal A's certificate and transmits PK.sub.a (X.sup.R.sbsp.b mod P) to terminal A. Terminal A receives and decrypts the message, obtains terminal B's public random component X.sup.R.sbsp.b mod P and exponentiates using its secret random component R.sub.a. **Terminal B receives and decrypts the message from terminal A, obtains terminal A's public random component X.sup.R.sbsp.a mod P and exponentiates it using its secret random component R.sub.b.**" Therefore, Examiner asserts that Faucher discloses a decryption operation.

Appellant further argues that “the entire protocol of column 8 of Faucher is performed in order to generate a session key, which is done by each terminal performing separate decryption operations of certification received from the other terminal. There is no joint performance of a joint decryption operation whereby each terminal performs subcomputations of the joint decryption operation. No where do the two Faucher terminals ‘jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party holds,’ as recited in the independent claims” (Page 8 of Appeal Brief).

Examiner respectfully disagrees. Faucher explicitly discloses the claimed limitation "performing of a joint decryption operation whereby each terminal performs subcomputations of the joint decryption operation” in Figure 5 and col. 8, lines 25-48, “For example, **terminal A sends its certificate to terminal B and terminal B sends its certificate to terminal A. Terminal A decrypts and validates terminal B's certificates using the KCA public decryption key. Similarly, terminal B decrypts and validates terminal A's certificate using the KCA public decryption key. Terminal A generates a secret random component R.sub.a, calculates the corresponding public component X.sup.R.sbsp.a mod P, encrypts it using the public encryption key PK.sub.b extracted from terminal B's certificate, and transmits PK.sub.b (X.sup.R.sbsp.a mod P) to terminal B. Terminal B generates a secret random component R.sub.b, calculates the corresponding public component X.sup.R.sbsp.b mod P, encrypts it using the public encryption key PK.sub.a extracted from terminal A's certificate and transmits PK.sub.a**

(X.sup.R.sbsp.b mod P) to terminal A. Terminal A receives and decrypts the message, obtains terminal B's public random component X.sup.R.sbsp.b mod P and exponentiates using its secret random component R.sub.a. The result modulus P is passed over the hash function to obtain the session key. **Terminal B receives and decrypts the message from terminal A obtains terminal A's public random component X.sup.R.sbsp.a mod P, and exponentiates it using its secret random component R.sub.b**. The result modulus P is passed over the hash function H to obtain the session key" (Faucher, col. 8, lines 25-48). Furthermore, Appellant has failed to explicitly identify specific claim limitation "the joint decryption operation" that would define a patentable distinction over prior art. Appellant merely mentions "the joint decryption operation" in the claim, but does not define metes and bounds of the term "the joint decryption operation." Examiner interprets the claim language in its broadest and reasonable meaning in view of the specification. The examiner interprets "the joint decryption operation" as **Terminal A generates a secret random component R.sub.a, calculates the corresponding public component X.sup.R.sbsp.a mod P, encrypts it using the public encryption key PK.sub.b extracted from terminal B's certificate, and transmits PK.sub.b (X.sup.R.sbsp.a mod P) to terminal B, when receives, terminal B decrypts the message from terminal A, obtains terminal A's public random component X.sup.R.sbsp.a mod P and exponentiates it using its secret random component R.sub.b** which can read on the claim limitation jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each

party holds. Therefore, Examiner asserts that the combination of Cramer and Faucher does teach or suggest the subject matter broadly recited in the independent claims and in subsequent dependent Claims.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., each perform one or more subcomputations of the ***singular*** decryption operation) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Appellant further argues that "Appellant maintains that the Examiner has failed to identify a cogent motivation for combining Cramer and Faucher in the manner proposed" (Page 9 of Appeal Brief).

Examiner respectfully disagrees with this contention. In response to appellant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and In re Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992), In this

case, Cramer's reference and Faucher's reference are analogous arts. They both specifically disclose to how to secure communications by using the cryptographic system that can support the motivation to combine the Cramer's teaching with Faucher's teaching to establish the limitations of Claim 1 that provides secure communications conducted over insecure channels (Faucher, col. 1, lines 13-15). Furthermore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Faucher's reference within Cramer to include wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device. One of ordinary skill in the art would have been motivated to do this because it would secure communications conducted over insecure channels using pubic-keys method (Faucher, col. 1, lines 13-15).

II. Regarding dependent Claims 2 and 10,

Appellant further argues that Cramer does not teach or suggest “exchange of information between the first party device and the second party device whereby at least a portion of the information is encrypted using an encryption technique such that one party encrypts information using its own public key and another party cannot read the information but can use the information to perform an operation” (Pages 9 and 10 of Appeal Brief).

Examiner respectfully disagrees. Faucher further discloses wherein the generating step further comprises an exchange of information between the first party device and the second party device whereby at least a portion of the information is encrypted using an

encryption technique such that one party encrypts information using its own public key and another party can not read the information but can use the information to perform an operation" (Faucher, Figure 5, col. 8, lines 8-55). Therefore, Examiner asserts that the combination of Cramer and Faucher discloses the limitations of Claims 2 and 10.

III. Regarding dependent Claims 4 and 12,

Appellant further argues that Cramer does not disclose or suggest "Cramer discloses generating a share of a random secret; generating information representing encryptions of a form of the random secret, a share of a private key, and the ciphertext; transmitting at least the encrypted information to the second party device; and computing the plaintext based at least on the share of the random secret, the share of the private key, the ciphertext, and the data received from the second party device" (Page 10 of Appeal Brief).

Examiner respectfully disagrees. Cramer discloses generating a share of a random secret (Col. 7, lines 11-19); generating information representing encryptions of a form of the random secret, a share of a private key, and the ciphertext (Col. 7 lines 10-27) {private key Z, and the random group}; transmitting at least the encrypted information to the second party device (Col. 6, lines 46-57); and computing the plaintext based at least on the share of the random secret, the share of the private key, the ciphertext, and the data received from the second party device (Figure 3, Col. 9 lines 25-50). Therefore, Examiner asserts that the combination of Cramer and Faucher discloses the limitations of 4 and 12.

IV. Regarding dependent Claims 6 and 14,

Appellant further argues that Cramer does not disclose or suggest "the first party device and the second party device additively share components of a private key" and "generation and exchange of proofs between the first party device and the second party device that serve to verify operations performed by each party" (Page 11 of Appeal Brief).

Examiner respectfully disagrees. Cramer discloses "the first party device and the second party device additively share components of a private key" in (Col. 7 lines 10-15, and Col. 9 lines 35-40); and generation and exchange of proofs between the first party device and the second party device that serve to verify operations performed by each party" in (Col. 8 line 38 to Col. 9 line 23). Therefore, Examiner asserts that the combination of Cramer and Faucher discloses the limitations of Claims 6 and 14.

V. Regarding dependent Claims 3, 7, 11, and 15,

Appellant further argues that "the Cramer paper reference fails to remedy the deficiencies described above with regard to Cramer and Faucher. Thus, claims 3, 7, 11, and 15 are patentable at least by virtue of their dependency from claims 1 and 9" (Page 11 of Appeal Brief).

Examiner respectfully disagrees because as discussed above, the combination of Cramer and Faucher discloses all the limitation of Claims 1 and 9. Therefore, Examiner asserts that the combination of Cramer, Faucher, and Faucher paper also discloses the limitations of Claims 3, 7, 11, and 15.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Baotran N. To/

Examiner, Art Unit 2435

Conferees:

/Beemnet W Dada/
Primary Examiner, Art Unit 2435

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435